Algorithmes pour compter des points de courbes en petite caractéristique et en petit genre

Jean-François Mestre

rédigé par David Lubicz

Soit C une courbe (hyperelliptique, mais ceci n'est pas essentiel) de genre g définie sur $\mathbb{F}_{2^d}$ et dont la jacobienne est ordinaire. On donne ici une méthode permettant de trouver le produit $\pi_1 \ldots \pi_g$ des valeurs propres inversibles (relativement à un idéal premier au-dessus de 2) du Frobenius.

Dans le cas du genre 1, on retrouve l'algorithme (dit depuis AGM) décrit initialement dans [1]. Dans le cas du genre 2, on obtient une méthode, aux formules plus simples que celle décrite également dans [1], et d'une complexité sensiblement égale, pour calculer le nombre de points de C sur $\mathbb{F}_{2^d}$.

1 Quelques suites convergeant rapidement

1.1 Rappels sur la moyenne arithmético-géometrique (MAG ou AGM)

Soient a, b deux nombres réels positifs, nous définissons par récurrence les suites a_n et b_n en posant :

$$(a_0, b_0) = (a, b), \tag{1}$$

$$(a_{n+1}, b_{n+1}) = (\frac{a_n + b_n}{2}, \sqrt{a_n b_n}). \tag{2}$$

Ces deux suites convergent alors vers une même limite notée $M(a,b)$ appelée moyenne arithmético-géométrique de a et b. Cette convergence est quadratique, c'est-à-dire qu'il existe une constante $\alpha \in \mathbb{R}$ telle que :

$$|b_n - a_n| \leq \alpha |b_{n-1} - a_{n-1}|^2.$$

Ces résultats ont été obtenus par Legendre et retrouvés par Gauss à l'âge de 13 ans.

1.2 La moyenne de Borchardt

Soient a, b, c, d quatres nombres réels positifs ; définissons par récurrence les suites a_n, b_n, c_n et d_n en posant :

$$(a,b,c,d) = (a_0, b_0, c_0, d_0) \tag{3}$$
$$a_{n+1} = \frac{a_n + b_n + c_n + d_n}{4}, \tag{4}$$
$$b_{n+1} = \frac{\sqrt{a_n b_n} + \sqrt{c_n d_n}}{2} \tag{5}$$
$$c_{n+1} = \frac{\sqrt{a_n c_n} + \sqrt{b_n d_n}}{2} \tag{6}$$
$$d_{n+1} = \frac{\sqrt{a_n d_n} + \sqrt{b_n c_n}}{2} \tag{7}$$

Ces quatre suites convergent alors quadratiquement vers une même limite appelée moyenne de Borchardt de a, b, c, d et notée $B(a,b,c,d)$.

1.3 Une généralisation

Soit G le groupe $(\mathbb{Z}/2\mathbb{Z})^g$. À toute famille $A_0 = (a^0_\tau)_{\tau \in G}$ de réels > 0 indicée par G, on associe la famille $A^1 = (a^1_\tau)_{\tau \in G}$ définie, pour $\tau \in G$, par

$$a^1_\tau = \frac{1}{2^n} \sum_{\sigma \in G} \sqrt{a^0_\sigma a^0_{\sigma+\tau}}.$$

Les suites (A^n) ainsi définies par récurrence convergent quadratiquement vers un même réel $M_g(A^0)$.

Pour $g = 1$, on retrouve l'AGM, et pour $g = 2$, la moyenne de Borchardt.

1.4 La situation pour les nombres p-adiques

Soit k un corps local d'inégale caractéristique et d'uniformisante π. Soient $a, b \in k$ tels que

$$\frac{a}{b} \equiv 1(8\pi),$$

alors si $x \equiv 1(8\pi)$ on pose $\sqrt{x} \equiv 1(4\pi)$ ce qui lève l'ambiguïté sur la racine. On pose alors :

$$a_{n+1} = \frac{a_n + b_n}{2} \tag{8}$$

$$b_{n+1} = b_n \sqrt{\frac{a_n}{b_n}} \tag{9}$$

et on obtient deux suites qui convergent quadratiquement vers $M(a, b) \in k$ d'après [?].

De la même manière, si l'on se donne $a, b, c, d \in k$ tels que

$$\frac{a}{b} \equiv \frac{a}{c} \equiv \frac{a}{d} \equiv 1(8\pi)$$

on peut définir de manière similaire des suites a_n, b_n, c_n, d_n utilisant les formules de Borchardt et en prenant la même convention pour définir la racine carrée. Ces suites convergent quadratiquement vers $B(a, b, c, d)$. On peut procéder de même pour la généralisation donnée au paragraphe 1.3.

2 Application au calcul des périodes d'une courbe elliptique

Rappelons le résultat de Gauss :

$$\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{\cos^2\theta + 2\sin 2\theta}} = \frac{\pi}{2M(1, \sqrt{2})}.$$

Plus généralement on a :

$$\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{a^2\cos^2\theta + b^2\sin 2\theta}} = \frac{\pi}{2M(a,b)},$$

ou bien après un changement de variable :

$$\int_0^{\infty} \frac{dt}{\sqrt{x(x+a^2)(x+b^2)}} = \frac{\pi}{2M(a,b)},$$

qui est une période de la courbe elliptique d'équation $y^2 = x(x+a^2)(x+b^2)$.

On peut interpréter géométriquement ces égalités : soit les courbes elliptiques d'équation $E_n : y_n^2 = x_n(x_n + a_n^2)(x_n + b_n^2)$ où a_n et b_n ont été définis en (8). Alors nous disposons d'une isogénie de degré deux $\phi : E_1 \to E_0$ donnée par les équations :

$$\begin{cases} x_0 = x_1 + \frac{a_1^2(a_1^2-b_1^2)}{x_1+a_1^2} \\ y_0 = y_1\left[1 - \frac{a_1^2(a_1^2-b_1^2)}{(x_1+a_1^2)^2}\right] \end{cases}$$

Et on a

$$\phi^*(\frac{dx_0}{y_0}) = \frac{dx_1}{y_1}. \tag{10}$$

Alors si l'on pose :

$$I_n = \int_0^{\infty} \frac{dx}{\sqrt{x(x+a_n^2)(x+b_n^2)}},$$

(10) implique que l'on a $I_0 = I_1 = \ldots = I_\infty$ avec

$$I_\infty = \int_0^{\infty} \frac{dx}{\sqrt{x}(x+M^2(a,b))} = \frac{\pi}{2M(a,b)}.$$

La moyenne arithmético-géométrique permet donc de calculer une suite de courbes elliptiques reliées par des isogénies de degré 2 :

$$E_0 \leftarrow E_1 \leftarrow \ldots \leftarrow E_\infty$$

avec E_∞ la courbe de genre 0 d'équation $y^2 = x(x+M^2(a,b))^2$.

2.1 Le point de vue de la géométrie analytique

On sait qu'une courbe elliptique est isomorphe en tant que variété analytique au quotient du plan complexe $\mathbb{C}$ par un réseau. Nous pouvons alors représenter l'application ϕ de la manière suivante :

$$E_1 = \frac{\mathbb{C}}{[\omega_0, 2\omega_0']} \to E_0 = \frac{\mathbb{C}}{[\omega_0, \omega_0']}, \tag{11}$$

$$\phi : z \mapsto z \tag{12}$$

Il est alors évident que $\phi^*(dz) = dz$, d'où une suite d'isogénies reliant les $E_n = \frac{\mathbb{C}}{[\omega_0, 2^n\omega_0']}$.

2.2 Le point de vue des fonctions Θ

Posons

$$\Theta_0(q) = \sum_{n\in\mathbb{Z}} q^{n^2} \quad \text{et} \quad \Theta_1(q) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2}. \tag{13}$$

On a

$$\begin{cases} \Theta_0^2(q^2) = \frac{1}{2}\left(\Theta_0^2(q) + \Theta_1^2(q)\right) \\ \\ \Theta_1^2(q^2) = \Theta_0^2(q)\Theta_1^2(q). \end{cases}$$

Cette dernière identité est facile à démontrer avec la formule $(a+b)^2 + (a-b)^2 = 2(a^2+b^2)$. Ainsi, si l'on pose $a = \Theta_0^2(q)$ et $b = \Theta_1^2(q)$, on a :

$$\Theta_0^2(q^{2^n}) = a_n, \tag{14}$$

$$\Theta_1^2(q^{2^n}) = b_n, \tag{15}$$

où a_n, b_n est la suite MGA. Remarquons que cela permet de retrouver facilement la convergence quadratique de MGA, en effet on a,

$$\Theta_0^2(q^{2^n}) - \Theta_1^2(q^{2^n}) = q^{2^n}(\ldots).$$

Si $|q| < 1$ alors $MAG(\Theta_0^2(q), \Theta_1^2(q)) = 1$. Pour tout $a, b \in \mathbb{Z}^+$, alors il existe $q \in \mathbb{C}$ avec $|q| < 1$ tel que

$$a = \Theta_0^2(q)\omega_0 \tag{16}$$

$$b = \Theta_1^2(q)\omega_0 \tag{17}$$

Comme $M(\lambda a, \lambda b) = \lambda M(a,b)$ on a $M(a,b) = \omega_0$.

2.3 Les fonctions Θ à plusieurs variables

Soit τ la matrice des périodes d'une courbe de genre g, alors τ est symétrique et $Im(\tau)$ est définie positive.

$$\Theta(\tau, z) = \sum_{n \in \mathbb{Z}^g} e^{\pi i^t n \tau n + 2\pi^t n z}.$$

Si $g = 2$, on a d'après [?] p. 118,123,222 : si l'on pose

$$\beta_0(\tau) = \Theta(\tau, (0,0)) \quad \beta_1 = \Theta(\tau, (1/2, 0)), \tag{18}$$

$$\beta_2(\tau) = \Theta(\tau, (0, 1/2)) \quad \beta_3 = \Theta(\tau, (1/2, 1/2)), \tag{19}$$

on a

$$\beta_0(2\tau)^2 = \frac{\beta_0^2(\tau) + \beta_1^2(\tau) + \beta_2^2(\tau) + \beta_3^2(\tau)}{4}, \tag{20}$$

$$\beta_1^2(2\tau) = \frac{\beta_0(\tau)\beta_1(\tau) + \beta_2(\tau)\beta_3(\tau)}{2}, \tag{21}$$

$$\beta_2^2(2\tau) = \frac{\beta_0(\tau)\beta_2(\tau) + \beta_1(\tau)\beta_3(\tau)}{2}, \tag{22}$$

$$\beta_3^2(2\tau) = \frac{\beta_0(\tau)\beta_3(\tau) + \beta_2(\tau)\beta_3(\tau)}{2}. \tag{23}$$

Et pour $i = 0, 1, 2, 3$, les $\beta_i(2^n\tau)$ tendent vers 1. Soit H une courbe hyperelliptique de genre 2 et l'on suppose qu'elle a pour équation : $y^2 = (x - e_1) \ldots (x - e_6)$ avec $e_6 < \ldots < e_1$ des nombres réels. On se donne la base $\{\frac{dx}{y}, \frac{xdx}{y}\}$ des différentielles régulières de H et $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ la base de $H_1(H, \mathbb{Z})$ associée à H comme dans [?], ch. 1. On peut alors former la matrice des périodes de H qui s'écrit sous la forme de deux blocs de matrices 2×2, $(\Omega\Omega')$. Maintenant, si l'on pose,

$$A = \sqrt{|(e_6 - e_4)(e_5 - e_2)(e_3 - e_1)|}, \tag{24}$$

$$B = \sqrt{|(e_6 - e_4)(e_5 - e_1)(e_3 - e_1)|}, \tag{25}$$

$$C = \sqrt{|(e_6 - e_3)(e_5 - e_2)(e_4 - e_1)|}, \tag{26}$$

$$D = \sqrt{|(e_6 - e_1)(e_5 - e_1)(e_4 - e_2)|}. \tag{27}$$

Le théorème généralise celui de Gauss :

Théorème 1 (Formule de Thomae, Fay, [?] ch. 1, paragraphe 8).

$$B(A, B, C, D) = \frac{4\pi^2}{det\Omega}.$$

3 Courbes sur un corps fini

Soit C une courbe algébrique projective lisse de genre g définie sur le corps $\mathbb{F}_q$ et soit J sa jacobienne. Notons $\pi_1, \pi_2, \ldots, \pi_g, \overline{\pi}_1, \ldots, \overline{\pi}_g$ les valeurs propres du morphisme de Frobenius. On a les formules

$$\sharp J(\mathbb{F}_q) = \prod_{i=1}^{g}(1-\pi_i)(1-\overline{\pi_i}), \tag{28}$$

$$\sharp C(\mathbb{F}_q) = q + 1 - \sum_{i=1}^{g}(\pi_i + \overline{\pi}_i). \tag{29}$$

3.1 Rappel du cas du genre 1

Il s'agit ici du rappel de la méthode donnée dans [1].

Rappelons d'abord le lemme suivant [**?**]

Lemme 1. Soit E une courbe elliptique définie sur un corps k de caractéristique 0 et soit $\omega \in \Omega^1(E)$; l'application $\lambda : \quad End_k(E) \to k$ qui a $f \in End_k(E)$ fait correspondre $\lambda_f = f^*(\omega)/\omega$ est un morphisme d'anneaux injectif. En particulier, on a

$$\lambda_{f^\vee} = \frac{\deg(f)}{\lambda_f}$$

et donc

$$Tr\ f = \lambda_f + \frac{\deg(f)}{\lambda_f}.$$

Soit maintenant E une courbe définie sur $\mathbb{F}_{2^d}$, dont on veut compter le nombre de points. Nous utilisons l'idée de Satoh qui consiste pour ce faire à calculer son relèvement canonique $\tilde{E}$ dans l'extension non ramifiée de degré d de $\mathbb{Q}_2$.

L'idée de l'algorithme est la suivante :

Considérons la suite d'isogénies

$$\tilde{E}_0 \leftarrow \tilde{E}_1 \leftarrow \ldots \leftarrow \tilde{E}_d,$$

les flèches correspondant au dual du petit Frobenius. On a alors $\tilde{E}_0 \simeq \tilde{E}_d$, cet isomorphisme étant donné par une isogénie ϕ entre les courbes :

$$y_d^2 = x_d(x_d - a_d^2)(x_d - b_d^2)$$

$$y_0^2 = x_0(x_0 - a_0^2)(x_0 - b_0^2),$$

et nous savons que :

$$\phi^*(\frac{dx_0}{y_0}) = \frac{dx_d}{y_d} = u^{-1}\frac{dx_0}{y_0},$$

avec u tel que $a_d = ua_0$ et $b_d = ub_0$. En effectuant le changement de variable :

$$x_d = u^2 x_0 \tag{30}$$

$$y_d = u^3 y_0 \tag{31}$$

on retrouve $\tilde{E}_0$ et donc u^{-1} est le Frobenius :

$$\sharp C(\mathbb{F}_q) = q + 1 - (\frac{a_0}{a_d} + 2^d \frac{a_d}{a_0}).$$

Bien sûr, on ne connaît pas *a priori* le relèvement canonique $\tilde{E}_0$ de E_0.

On part d'un relèvement quelconque $E_0^\vee$ de la courbe E de la forme

$$y^2 = x(x - a^2)(x - b^2),$$

et l'on suppose que la valuation de $\frac{a}{b} - 1$ est égale à 3, ce qui revient à dire que la courbe est à réduction ordinaire.

Puis on construit la suite de courbes $(E_n^\vee)$ obtenue à partir de $E_0^\vee$ par les formules de la moyenne arithmético-géométrique. Alors l'invariant modulaire des courbes $(E_{nd}^\vee)$ converge vers celui du relèvement canonique de E.

Remarquons qu'ici nous ne sommes pas dans le cadre décrit dans la section 1.4 : les suites (a_n) et (b_n) ne sont pas convergentes ; néanmoins l'invariant modulaire des courbes $y^2 = x(x - a_n^2)(x - b_n^2)$ converge (linéairement, et non pas quadratiquement) vers l'invariant modulaire du relèvement canonique de E.

3.2 Le cas du genre 2

On se donne une extension k non ramifiée de degré d de $\mathbb{Q}_2$. Une courbe X de genre 2 définie sur $\mathbb{F}_{2^d}$ et dont la jacobienne est ordinaire se relève en une courbe de la forme :

$$Y^2 = (x - e_1) \dots (x - e_6),$$

avec

$$e_1 \equiv e_2, \quad e_3 \equiv e_4 \quad \text{et} \quad e_5 \equiv e_6 \mod 2.$$

Posons :

$$A = \sqrt{(e_1 - e_3)(e_3 - e_5)(e_5 - e_1)(e_2 - e_4)(e_4 - e_6)(e_6 - e_2)}, \tag{32}$$
$$B = \sqrt{(e_1 - e3)(e_3 - e_6)(e_6 - e_1)(e_2 - e_4)(e_4 - e_5)(e_5 - e_2)}, \tag{33}$$
$$C = \sqrt{(e_1 - e_4)(e_4 - e_5)(e_5 - e_1)(e_2 - e_3)(e_3 - e_6)(e_6 - e_2)}, \tag{34}$$
$$D = \sqrt{(e_1 - e_4)(e_4 - e_6)(e_6 - e_1)(e_2 - e_3)(e_3 - e_5)(e_5 - e_2)}, \tag{35}$$

en prenant les racines carrés évidentes, (A_n, B_n, C_n, D_n) est une suite convergente d'éléments de k. Si l'on pose

$$u = \frac{A_0}{A_d} = \frac{B_0}{B_d} = \frac{C_0}{C_d} = \frac{D_0}{D_d},$$

avec une précision de d chiffres, on a (voir le théorème de la section suivante)

$$u = \pi_1 \pi_2,$$

$$u \not\equiv 0((\pi)).$$

On connaît donc $\pi_1\pi_2$, ce qui bien sûr ne permet pas de déterminer de façon unique le couple (π_1, π_2), puisque par exemple $(-\pi_1, -\pi_2)$ donne le même produit $\pi_1\pi_2$.

Mais c'est en général la seule ambiguïté, et on peut trouver le polynôme caractéristique de la courbe en procédant comme suit :

Posons

$$b = (\pi_1 + \overline{\pi}_1)(\pi_2 + \overline{\pi}_2),$$

$$a = \pi_1 + \overline{\pi}_1 + \pi_2 + \overline{\pi}_2.$$

On a $|b| \leq 4q$ et $|a| \leq 4\sqrt{q}$. Comme

$$b - u = q(\frac{\pi_1}{\pi_2} + \frac{\pi_2}{\pi_1}) + \frac{q^2}{u} \tag{36}$$

on a $b \equiv u \mod q$. De plus, si l'on pose

$$\lambda = \frac{b-u}{q}$$

on a

$$\lambda \equiv \frac{\pi_1}{\pi_2} + \frac{\pi_2}{\pi_1}(q) \equiv \frac{\pi_1^2 + \pi_2^2}{u} \equiv \frac{a^2 - 2u}{u} \mod q \tag{37}$$

et donc $a^2 \equiv (\lambda + 2)u \mod q$.

3.3 Le cas du genre quelconque

Tout ceci se généralise au cas d'une variété abélienne ordinaire de dimension g définie sur $\mathbb{F}_q$, où $q = 2^d$, permettant ainsi de calculer le produit $\pi_1 \dots \pi_g$ des valeurs propres du Frobenius inversibles $\mod 2$.

Dans le cas d'une courbe hyperelliptique à jacobienne ordinaire définie sur $\mathbb{F}_q$, on la relève dans une extension de $\mathbb{Q}_2$ de façon à l'écrire $y^2 = p_1 \dots p_{g+1}$, où les p_i sont des polynômes de degré deux, premiers entre eux deux-à-deux $\mod 2$ et qui ont une racine double $\mod 2$.

À chaque ensemble de g parties ordonnées $\{x_2, x_2'\}, \dots, \{x_{g+1}, x_{g+1}'\}$ des racines de $p_2, \dots, p_{g+1}$, on associe les quantités $\sqrt{\prod_{1 \leq i < j \leq g+1}(x_i - x_j)(x_i' - x_j')}$, où l'on choisit les racines carrées de telle façon qu'elles soient congrues entre elles $\mod 4$. On considère alors la suite (A^n) définie dans la section 1.3, où $A^0 = (a_i)_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$ est la suite qu'on vient de définir, que l'on a indicé par $(Z/2\mathbb{Z})^g$.

On a alors la généralisation suivante des cas du genre 1 et du genre 2 décrits plus haut :

Théorème 2. Pour tout $i \in (\mathbb{Z}/2\mathbb{Z})^g$, La suite $A_i^{nd}/A_i^{(n+1)d}$ converge, quand n tend vers l'infini, vers un élément de $\mathbb{Z}_2$ égal au produit $\pi_1 \dots \pi_g$ des valeurs propres du Frobenius inversibles $\mod 2$.

Ce théorème ne fournit pas, au moins directement, le polynôme caractéristique du Frobenius $P = x^g + \dots$ dont les racines sont les $\pi_i + q\pi_i^{-1}$, $1 \leq i \leq g$.

Dans le cas du genre 1 et 2, il permet néanmoins de le trouver, comme on l'a vu plus haut.

Dans le cas général, notons $\alpha = \pi_1 \dots \pi_g$. Alors l'élément $\beta = \alpha + q^g/\alpha$ de $\mathbb{Z}_2$ est racine du polynôme P_{sym} unitaire à coefficients dans $\mathbb{Z}$ de degré 2^{g-1} dont les racines sont les $x + q^g/x$, où x décrit les produits de g termes appartenant chacun à $\{\pi_1, \overline{\pi_1}\}, \dots, \{\pi_g, \overline{\pi_g}\}$. De plus, β est l'unique racine de P_{sym} qui est une unité 2-adique.

La connaissance de P_{sym} entraîne essentiellement celle des π_i (puisqu'on connaît alors par exemple $\pi_1 \dots \pi_g$ et $\pi_1 \overline{\pi_2 \dots \pi_g}$, soit $q^{g-1}\pi_1^2$, etc.) et donc celle de P.

Par ailleurs, si P_{sym} est irréductible, la connaissance de α détermine P_{sym}, qui est le polynôme minimal de β. Pour trouver le polynôme minimal P_{min} de β, on peut par exemple employer une version 2-adique de LLL. S'il est de degré 2^{g-1}, il est égal à P_{sym}, et on peut donc en déduire le polynôme caractéristique $P(X)$ (ou $P(-X)$). Même lorsqu'il n'est pas de degré 2^{g-1}, le polynôme P_{min} permet souvent de retrouver le polynôme P, comme on va le voir ci-dessous.

1) Dans le cas du genre 2, si la jacobienne de C n'est pas (isogène au) carré d'une courbe elliptique, alors P_{sym} est irréductible.

Ceci provient du lemme suivant, qui prouve plus généralement que si β est dans $\mathbb{Z}$, la jacobienne de C est (isogène à) la puissance g-ième d'une courbe elliptique :

Lemme 2. Soit A une variété abélienne définie sur $\mathbb{F}_q$, de valeurs propres du Frobenius $\{\pi_1, \overline{\pi_1}, \dots, \pi_g, \overline{\pi_g}\}$. Soit $K = \mathbb{Q}(\pi_1, \dots, \pi_g)$; on suppose qu'il existe un idéal premier Q de K au-dessus de 2 tel que $\alpha = \pi_1 \dots \pi_g$ soit une unité Q-adique, et que $\beta = \alpha + \overline{\alpha}$ est un élément de $\mathbb{Z}$. Il existe alors une courbe elliptique E sur $\overline{\mathbb{F}_q}$ telle que A est $\overline{\mathbb{F}_q}$-isogène à E^g.

En effet, pour tout $1 \leq i, j \leq g$, notons $z_{ij} = \pi_i/\pi_j$. Comme $\beta \in \mathbb{Z}$, le groupe de Galois $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ laisse stable la partition $\{\pi_1, \dots, \pi_g\} \cup \{\overline{\pi_1}, \dots, \overline{\pi_g}\}$ (par exemple pour des raisons de valuation Q-adique) et l'ensemble $\{z_{ij}\}$, $1 \leq i, j \leq g$ est un ensemble stable par $G_{\mathbb{Q}}$ de nombres algébriques, entiers en-dehors de 2, entiers Q-adiques, donc en fait entiers algébriques, et de module 1. Ce sont donc des racines de l'unité, ce qu'il fallait démontrer.

Donc, dans le cas du genre 2, si P_{sym} n'est pas irréductible, i.e. si β est un élément de $\mathbb{Z}$, et on a $\pi_2 = z\pi_1$, où z est une racine de l'unité (d'ordre au plus 12), soit $\alpha = z\pi_1^2$. Par suite, pour le genre 2, α détermine dans tous les cas $Jac(C)$ à isogénie près.

2) En genre 3, comme on vient de le voir, si β est dans $\mathbb{Z}$, la jacobienne de C est isogène à E^3, E courbe elliptique ; pour des raisons analogues, si β est de degré 2, elle est isogène à $E^2 \times F$, E et F courbes elliptiques. Par contre, il existe des courbes C de genre 3 dont la jacobienne est absolument simple et telles que β est de degré 3 ; par exemple, $x^3 - 2x^2 - 6x + 11$ est le polynôme caractéristique d'une variété abélienne sur $\mathbb{F}_2$ absolument simple de dimension 3. Le polynôme P_{sym} associé est $(z+2)(z^3+9z^2+14z-28)$, donc le polynôme minimal de β est le polynôme de degré 3 $z^3 + 9z^2 + 14z - 28$.

Ceci est sans conséquence sur l'obtention à partir de α du polynôme caractéristique du Frobenius, car si le polynôme minimal de β est de degré 3, ses racines permettent d'obtenir tous les produits de trois valeurs propres du Frobenius sauf par exemple $\pi_1\pi_2\overline{\pi_3}$ et son conjugué, donc, par multiplication de termes de la forme $\pi_1\pi_2\pi_3$ et $\pi_1\overline{\pi_2\pi_3}$, détermine les π_i^2, $1 \leq i \leq 3$.

En particulier, si C est de genre 3, α détermine $Jac(C)$ à isogénie près.

3) Ce n'est plus le cas en dimension 4 : Soit A_1 et A_2 les deux variétés abéliennes ordinaires définies sur $\mathbb{F}_2$ de polynômes caractéristiques $P_1 = x^4 - 10x^2 - x + 19$ et $P_2 = x^4 - x^3 - 10x^2 + 8x + 17$. Le pgcd de $P_{1,sym}$ et $P_{2,sym}$ est $X^4 - 9X^3 - 24X^2 + 256X + 64$, dont l'unique racine unité 2-adique est le produit β des valeurs propres inversibles du Frobenius agissant sur A_1 et A_2, et A_1 et A_2 ont même α. Plus précisément, si $\pi_1, \overline{\pi_1}, \ldots, \pi_4, \overline{\pi_4}$ sont les valeurs propres du Frobenius de A_1, les carrés de celles de A_2 sont de la forme $\pi_2\pi_3\pi_4/\pi_1$, etc.

Par suite, en dimension 4, il peut arriver, même si c'est rare, que α ne détermine pas la variété abélienne à isogénie près.

Remarques.- 1) La complexité de la méthode suggérée ci-dessus pour calculer α est en 2^g, ce qui la rend inopérante pour g un peu grand, comparée notamment aux méthodes de Kedlaya et de Lauder et Wan.

2) Pour une courbe non hyperelliptique ou une variété abélienne en général, la méthode ci-dessus s'applique également, mais il faut savoir calculer les 2^g composantes du premier terme A^0 de la suite (A^n) en fonction du ou des polynômes

définissant la courbe ; il ne semble pas que dans la littérature figurent pour le cas non hyperelliptique des formules aussi utilisables que celles de Thomae.

[1] : J.-F. Mestre, lettre adressée à Gaudry et Harley, Déc. 2000, www.math.jussieu.fr/~mestre